DETAILED ACTION

1. A **Request for Continued Examination** under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on **20 October 2010** has been entered.

2. **Claims 1-8, 10-12, 14-26** remain **rejected**.

Responses to the Argument

3. Applicant's arguments, see page 14, filed 20 October 2010 with respect to the rejection(s) of claim(s) **1-8, 10-12, 14-26** under **35 USC § 103** have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Godwin.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 22-24 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims recite "a **computer-readable storage medium**, but computer-readable medium is not defined in the specification of the application. Pending claims are interpreted as broadly as their terms reasonably allow. See In re Zletz, 893 F.2d 319 (Fed. Cir. 1989). The broadest reasonable interpretation of a claim drawn to a computer readable medium (also called machine readable medium and other such variations) typically covers forms of non-transitory tangible media and transitory propagating signals per se in view of the ordinary and customary meaning of computer readable media, particularly when the specification is silent (See MPEP 2111.01). When the broadest reasonable interpretation of a claim covers a **signal per se**, the claim must be rejected under 35 U.S.C. §101 as covering non-statutory subject

matter. See In re Nuijten, 500 F.3d 1346, 1356-57 (Fed. Cir. 2007) (transitory embodiments are not directed to statutory subject matter) and Interim Examination Instructions for Evaluating Subject Matter Eligibility Under 35 U.S.C. § 101, Aug. 24, 2009; p. 2.

A claim drawn to such a computer readable medium that covers both transitory and non-transitory embodiments may be amended to narrow the claim to cover only statutory embodiments to avoid a rejection under 35 U.S.C. § 101 by adding the limitation "non-transitory" to the claim. Cf. Animals – Patentability, 1077 Off. Gaz. Pat. Office 24 (April 21, 1987.

Claim Rejections - 35 USC § 112

5. "An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof."

Claims 25 and **26** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The word "means" is preceded by the word(s) "means for issuing, means for communicating, means for providing, means for receiving, in an attempt to use a "means" clause to recite a claim element as a means for performing a specified function. However, since no function is specified by the word(s) preceding "means," it is impossible to determine the equivalents of the element, as required by 35 U.S.C. 112, sixth paragraph. See Ex parte Klumb, 159 USPQ 694 (Bd. App. 1967). Examiner could not determine the proper structure and algorithm for each limitations of "means for" in the claims as it is required if applicant invoking 112/6th paragraph.

The examiner notes to the applicant that can overcome the rejection by executing one of the following options: 1) point the examiner where in applicants specification applicant structure and algorithm for invoking the means plus function rule, 2) strike the means plus function claim language from the claim, 3) cancel the claim.

Claim Rejections - 35 USC § 103

4 The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-8, 10-12 and **14-26** are rejected under **35 U.S.C §103(a)** as being unpatentable over U.S. Patent No. 6,760,444, hereinafter Leung and in view of Godwin et al (US Publication No. 20020133608), hereinafter Godwin.

In regard to **claim 1**, Leung discloses:

- **an application device** (Leung, col 6, lines 24-26).

- a service device (Leung, col2, line 58 to column 3, line 16), wherein The Home Agent is the service device.

- a communication network configured to connect said application device to said service device (Leung, col 6, lines 24-26), wherein the home agent and handheld device are connected via communication network.

- an internet protocol security service unit configured to provide one or more internet protocol security services comprising at least one of authentication services and encryption services, said internet protocol security service unit deployed in said service device (Leung, col 6, lines 24-26, col 2, lines 58 and col 3, lines 16) wherein, The Home Agent may contact the server with a request for services such as creating and managing security associations or authentication services handled by the server's internet protocol security services.

- a management server configured to receive said security association management requests issued from said at least one management client and to respond, in connection with said internet protocol security service unit, to said security association management

requests received at said management server, said management server deployed in said service device The Home Agent may contact the server with a request for services such as creating (Leung, col 2, line 58, col 3, line 16) and managing security associations or authentication services (handled by the server's internet protocol security services) and receive in return a security association (Leung column 7, lines 16-32). The response is sent by the server to the home agent (Leung col 7, lines 33-50), since the security associations may comprise keys (Leung column 7, line 67), this uses a session key management protocol.

- at least one management client configured to issue, in response to communication received at said application device from a user equipment via a session key management protocol, The response is sent by the server to the home agent (Leung col 7, lines 33-50), since the security associations may comprise keys (Leung col 7, line 67), this uses a session key management protocol.

Leung does not explicitly teach **security association management requests to create and manage, with said session key management protocol, security associations for use by said provided internet protocol security services, said at least one management client deployed in said application device ;** however in a relevant art Godwin teaches this functionality (Godwin, ¶28-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the encrypted authentication of Leung with the create and manage request associated with the session key negotiation disclosed in Godwin, since the present invention provides for adaptive network security. Encryption with key negotiation provides extra layer of data protection.

In regard to **claim 2, 11,** and **19:**

The Home Agents network interface for communicating with the communications network, see col 9, line 53 to col 10, line 6, provides communication between the management clients and the server.

In regard to **claim 3, 12, 15**

- wherein said security association is taught by Leung see figure 4, item 412. but Leung does not explicitly teach **management requests to create and manage comprise at least one of adding requests configured to add security associations, deleting requests configured to delete security associations, and querying requests configured to query about security associations;** however in a relevant art Godwin teaches this functionality (Godwin, ¶28-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the encrypted authentication of Leung with the create and manage request associated with the session key negotiation disclosed in Godwin, since the present invention provides for adaptive network security. Encryption with key negotiation provides extra layer of data protection.

In regard to **claim 16**, Leung discloses:

a management server configured to receive security association management requests issued from at least one management client included in an application device external to said apparatus and to respond, in connection with said internet protocol security service unit, to said received security association management requests to create and manage security associations The Home Agent may contact the server with a request for services such as creating (Leung, col 2, line 58, col 3, line 16) and managing security associations or authentication services (handled by the server's internet protocol security services) and receive in return a security association (Leung column 7, lines 16-32). The response is sent by the server to the home agent (Leung col 7, lines 33-50), since the security associations may comprise keys (Leung column 7, line 67), this uses a session key management protocol. Mobile node is the individual computing device (Abstract).

Leung does not explicitly teach **requests to create and manage ;** however in a relevant art Godwin teaches this functionality (Godwin, ¶28-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the encrypted authentication of Leung with the create and manage request associated with the session key negotiation disclosed in Godwin, since the present invention provides for adaptive network security. Encryption with key negotiation provides extra layer of data protection.

In regard to **claim 4** and **5:**

the server may use IP, for which all communications inherently use sockets at both ends of a communication and data structures for the packet formats (Leung, col 6, lines 26-28 and col 8, lines 37-39).

In regard to **Claims 6, 7, 9,** and **17**:

Regarding **claim 6**, Leung does not discuss the architecture of the software in the system that is employed to use the communications interface.

Official notice is given that it is well-known in the art to package the related functions for using a device on a computer in a DLL.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to implement the network interface functions as a DLL.

Regarding **claims 7, 9,** and **17** Leung does not disclose the structure of the network connecting the Home Agents to the servers.

Official notice is given that it is well-known in the art to implement computer connections using a local network.

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement Leung's invention using a local network.

In regard to **claim 8:**

Each client's security associations and communications may use a different keying algorithm (Leung, FIG.4, item 412).

In regard to **claim 10**, Leung discloses:

- providing one or more internet protocol security services comprising at least one of authentication services and encryption services from an internet protocol security service unit, said internet protocol security service unit being deployed in a service device (Leung, col 2, line 58 to col 3, line 16) The Home Agent may contact the server with a request for

services such as creating and managing security associations or authentication services (handled by the server's internet protocol security services.

- receiving in a management server said security association management requests issued from said at least one management client (Leung col 7, lines 16-32), wherein receive in return a security association.

- and responding, in connection with said internet protocol security service unit, to said security association management requests received at said management server, said management server being deployed in said service device, wherein said application device is connected to said service device by a communication network Leung discloses an interaction between a Home Agent the application device comprising management clients that is connected to a server (the service device) via a communications network (Leung col 6, lines 24-26) and one or more wireless clients. The Home Agent may contact the server with a request for services such as creating (Leung col 2, line 58 to col 3, line 16) and managing security associations or authentication services (handled by the server's internet protocol security services) and receive in return a security association (Leung col 7, lines 16-32). The response is sent by the server to the home agent (Leung column 7, lines 33-50), since the security associations may comprise keys (col column 7, line 67), this uses a session key management protocol.

- issuing, in response to communication received at an application device from a user equipment via a session key management protocol (Leung, figure 4, item 412).

Leung does not explicitly teach **security association management requests to create and manage, with said session key management protocol, security associations for use by said provided internet protocol security services, from at least one management client, said at least one management client being deployed in said application device;** however in a relevant art Godwin teaches this functionality (Godwin, ¶28-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the encrypted authentication of Leung with the create and manage request associated with the session key negotiation disclosed in Godwin, since the present invention provides for adaptive network security. Encryption with key negotiation provides extra layer of data protection.

In regard to **claim 14,** Leung discloses:

Leung discloses an interaction between a Home Agent the application device comprising management clients, that is connected to a server (the service device) via a communications network (Leung, col 6, lines 24-26) and one or more wireless clients. The Home Agent may contact the server with a request for services such as creating (Leung, col 2, line 58 to column 3, line 16) and managing security associations or authentication services (handled by the server's internet protocol security services) and receive in return a security association (Leung, col 7, lines 16-32). The response is sent by the server to the home agent (Leung, col 7, lines 33-50), since the security associations may comprise keys (Leung, col 7, line 67), this uses a session key management protocol.

Wherein the at least one management client is included in an application device Mobile node is the individual computing device (Abstract).

Leung does not explicitly teach **requests to create and manage;** however in a relevant art Godwin teaches this functionality (Godwin, ¶28-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the encrypted authentication of Leung with the create and manage request associated with the session key negotiation disclosed in Godwin, since the present invention provides for adaptive network security. Encryption with key negotiation provides extra layer of data protection.

In regard to **claim 18**, Leung discloses:

Leung discloses managing security associations or authentication services (handled by the server's internet protocol security services) and receive in return a security association (Leung, col 7, lines 16-32). The response is sent by the server to the home agent (Leung, col 7, lines 33-50), since the security associations may comprise keys (Leung, col 7, line 67), this uses a session key management protocol.

Leung discloses an interaction between a Home Agent the application device comprising management clients, that is connected to a server (the service device) via a communications network (Leung, col 6, lines 24-26) and one or more wireless clients. The Home Agent may

contact the server with a request for services such as creating (Leung, col 2, line 58 to column 3, line 16).

Leung does not explicitly teach **requests to create and manage;** however in a relevant art Godwin teaches this functionality (Godwin, ¶28-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the encrypted authentication of Leung with the create and manage request associated with the session key negotiation disclosed in Godwin, since the present invention provides for adaptive network security. Encryption with key negotiation provides extra layer of data protection.

In regard to **claim 19,** Leung discloses:

- wherein said communicating comprises communicating at least one of said security association management requests issued from said application device and corresponding responses via an interface associated with said application device (Leung col 6, lines 24-26), a server (the service device) via a communications network and one or more wireless clients.

In regard to **claim 20**, claim 18 is incorporated and Leung discloses:

- wherein said issuing comprises issuing said security association management requests comprising at least one of adding requests for adding security associations, deleting requests for deleting security, and querying requests for querying about security associations (Leung, col 6, lines 26-28 and col 8, lines 37-39), wherein security associations must be copied from the server to the Home Agent in order to create and manage or facilitate modifications in security associations.

In regard to **claim 21**, Leung discloses:

- providing one or more internet protocol security services comprising at least one of authentication services and encryption services from an internet protocol security service unit, wherein said internet protocol security service unit is deployed in a service device (Leung, col 6, lines 29-36, "In addition to providing a centralized server which is capable of storing security-associations for multiple Home Agents, the centralized server may provide

further services. By way of example, the centralized server may provide authentication services and/or authorization services. While authentication determines who an entity is, authorization determines what services a user is allowed to perform, or access");

Leung does not explicitly teach **- receiving means for receiving security association management requests to create and manage security association, the security association management requests issued from at least one management client included in an application device external to said apparatus and for responding, in connection with said internet protocol security service means, to said received security association management requests**; however in a relevant art Godwin teaches this functionality (Godwin, ¶28-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the encrypted authentication of Leung with the create and manage request associated with the session key negotiation disclosed in Godwin, since the present invention provides for adaptive network security. Encryption with key negotiation provides extra layer of data protection.

In regard to **claim 22**, Leung discloses:

- providing one or more internet protocol security services comprising at least one of authentication services and encryption services from an internet protocol security service unit, said internet protocol security service unit being deployed in a service device (Leung, col 6, lines 29-36, "In addition to providing a centralized server which is capable of storing security-associations for multiple Home Agents, the centralized server may provide further services. By way of example, the centralized server may provide authentication services and/or authorization services. While authentication determines who an entity is, authorization determines what services a user is allowed to perform, or access");

- issuing security association management requests to create and manage, with a session key management protocol, security associations for use by said provided internet protocol security services, from at least one management client, said at least one management client being deployed in an application device (Leung, col 7, lines 54-61, "The security association may be retrieved from the server each time mobile node 702 sends a fresh

registration request. To reduce the effort associated with this, the security association may be temporarily loaded into memory (e.g., a portion of DRAM) of the Home Agent. In this manner, some transfers of security associations from the server to the Home Agent are eliminated");

- receiving in a management server said security association management requests issued from said at least one management client (Leung, col 7, lines 35-47, "At step 714, the server receives the packet identifying the mobile node (e.g., an authorization request packet) from the Home Agent. … ..appropriate format (e.g., a TACACS+ authorization reply packet) and includes the security association").

- responding, in connection with said internet protocol security service unit, to said security association management requests received at said management server, said management server being deployed in said service device, wherein said application device is connected to said service device by a communication network (Leung, col 4, lines 33-45, "While authentication determines who an entity is, authorization determines what services a user is allowed to perform, or access. … available at http://www.ietf.org/internet-drafts/draft-grant-tacacs-02.txt, describes").

Leung does not explicitly teach **requests to create and manage**; however in a relevant art Godwin teaches this functionality (Godwin, ¶28-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the encrypted authentication of Leung with the create and manage request associated with the session key negotiation disclosed in Godwin, since the present invention provides for adaptive network security. Encryption with key negotiation provides extra layer of data protection.

In regard to **claim 23**, Leung discloses:

- issuing, from at least one management client deployed in an application device, security association management requests to create and manage, with a session key management protocol, security associations for use by one or more internet protocol security services comprising at least one of authentication services and encryption services provided by an internet protocol security service unit external to said application device (Leung, col 7, lines 62-68, "A suitable algorithm for clearing security associations from the

Home Agent's memory may be employed (e.g., a least recently used (LRU) algorithm). While this approach can reduce traffic between server and Home Agent--and thereby eliminate attendant delay--it must also account for modifications of security associations (e.g., keys) on the server");

- communicating at least one of said issued security association management requests to a management server external to said application device, said management server configured to respond to said security association management requests in connection with said internet protocol security service unit (Leung, col 10, lines 18-24, "an architecture having a single processor that handles communications as well as routing computations, etc. would also be acceptable. Further, other types of interfaces and media could also be used with the router. Still further, in some cases, the invention can be implemented on network devices other than routers").

Leung does not explicitly teach **requests to create and manage**; however in a relevant art Godwin teaches this functionality (Godwin, ¶28-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the encrypted authentication of Leung with the create and manage request associated with the session key negotiation disclosed in Godwin, since the present invention provides for adaptive network security. Encryption with key negotiation provides extra layer of data protection.

In regard to **claim 24**, Leung discloses:

- providing one or more internet protocol security services comprising at least one of authentication services and encryption services from an internet protocol security service unit, said internet protocol security service unit being deployed in a service device (Leung, col 8, lines 17-26, "FIG. 8 is a process flow diagram illustrating the steps performed .. server are illustrated along vertical line 806. Again, the server is preferably an AAA server that can provide authorization and accounting services as well as authentication services");

Leung teaches **included in an application device** (Abstract). But Leung does not explicitly teach **- receiving means for receiving security association management requests to create and manage security association, the security association management requests**

issued from at least one management client included in an application device external to said apparatus and for responding, in connection with said internet protocol security service means, to said received security association management requests; however in a relevant art Godwin teaches this functionality (Godwin, ¶28-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the encrypted authentication of Leung with the create and manage request associated with the session key negotiation disclosed in Godwin, since the present invention provides for adaptive network security. Encryption with key negotiation provides extra layer of data protection.

In regard to **claim 25**, Leung discloses:

- managing means for issuing security association management requests to create and manage, with a session key management protocol, security associations for use by one or more internet protocol security services comprising at least one of authentication services and encryption services provided by an internet protocol security service means external to said apparatus (Leung, col 7, lines 35-47, "At step 714, the server receives the packet identifying the mobile node (e.g., an authorization request packet) from the Home Agent…the security association").

- communicating means for communicating said issued security association management requests to a management server external to said apparatus, said management server configured to respond to said security association management requests in connection with said internet protocol security service means (Leung, col 10, lines 18-24, "an architecture having a single processor that handles communications as well as routing computations, etc. would also be acceptable. Further, other types of interfaces and media could also be used with the router. Still further, in some cases, the invention can be implemented on network devices other than routers").

- **wherein the apparatus is included in an application device ,** wherein Mobile node is the individual computing device (Abstract).

Leung does not explicitly teach **requests to create and manage**; however in a relevant art Godwin teaches this functionality (Godwin, ¶28-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the encrypted authentication of Leung with the create and manage request associated with the session key negotiation disclosed in Godwin, since the present invention provides for adaptive network security. Encryption with key negotiation provides extra layer of data protection.

In regard to **claim 26**, Leung discloses:

- **internet protocol security service means for providing one or more internet protocol security services comprising at least one of authentication services and encryption services** (Leung, col 6, lines 32-36, "the centralized server may provide authentication services and/or authorization services. While authentication determines who an entity is, authorization determines what services a user is allowed to perform, or access");

Leung does not explicitly teach **- receiving means for receiving security association management requests to create and manage security association, the security association management requests issued from at least one management included in an application device client external to said apparatus and for responding, in connection with said internet protocol security service means, to said received security association management requests**; however in a relevant art Godwin teaches this functionality (Godwin, ¶[28-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the encrypted authentication of Leung with the create and manage request associated with the session key negotiation disclosed in Godwin, since the present invention provides for adaptive network security. Encryption with key negotiation provides extra layer of data protection.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure (see form "PTO-892 Notice of Reference Cited").

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Monjour Rahim whose telephone number is (571)270-3890. The examiner can normally be reached on 7:00 AM -5:00 PM (Mo-Th).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Thomas can be reached on 571-273-6776. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (in USA or CANADA) or 571-272-1000.

/Monjour Rahim/
Patent Examiner
Art Unit: 2492
Date: 12/27/2010

/JOSEPH THOMAS/
Supervisory Patent Examiner, Art Unit 2492